THE BROOKINGS INSTITUTION

WEBINAR

ASIA TRANSNATIONAL THREATS FORUM:
CYBERSECURITY AND CYBER RESILIENCE

Washington, D.C.

Thursday, October 29, 2020

PARTICIPANTS:

Welcoming Remarks:

JOHN ALLEN
President
The Brookings Institution

Keynote Address:

BAE JONGIN
Ambassador for International Security Affairs and
Special Advisor to the Minister of Foreign Affairs
Ministry of Foreign Affairs
Republic of Korea

Panelists:

JUNG H. PAK
Senior Fellow and SK-Korea Foundation Chair in Korea
Studies, Center for East Asia Policy Studies
The Brookings Institution

MIHOKO MATSUBARA
Chief Cybersecurity Strategist
NTT Corporation

ELINA NOOR
Director, Political-Security Affairs and Deputy
Director, Washington, D.C. Office,
Asia Society Policy Institute

THOMAS UREN
Senior Analyst, International Cyber Policy Centre,
Australian Strategic Policy Institute

* * * * *

P R O C E E D I N G S

GENERAL ALLEN: Ladies and gentlemen, good morning, good afternoon, good evening from wherever you're tuning in today around the world. My name is John Allen. I'm the president of the Brookings Institution and it is my great pleasure to welcome you all to the Asia Transnational Threats Forum: Cybersecurity and Cyber Resilience.

Before we begin, I'd to thank the first to thank, the Korea Foundation for their generous support in making this event possible. Their partnership with us has been long and productive and continues to be invaluable to our research on all things related to the peninsula. Today's conference is the fourth iteration of the Asia Transnational Threats Forum or ATTF as it's called. And this series has been very important to so many of us.

Since its launch by our Center for East Asia Policy Studies in 2018, the ATTF has convened to examine strategic challenges affecting all of Asia, including counter terrorism and climate change. This year, the focus will be on cybersecurity issues in Asia and the impact of digital technologies on regional security, economics and political dynamics. Moderated by Brookings senior fellow and SK-Korea Foundation chair in Korean Studies, Jung Pak. We are excited to have a distinguished line up of experts from across the Pacific who will present and discuss the current cyber threat environment and the cybersecurity ecosystem in the region.

So, to kick off the event, we're especially honored to welcome Ambassador Jongin Bae of the Republic of Korea. Since joining the Ministry of Foreign Affairs in 1992, Ambassador Bae has served overseas in various roles in Northeast Asia, North America, and Africa, including deputy director general of Northeast Asian Affairs Bureau.

In his current capacity as the ambassador for International Security Affairs, Ambassador Bae has been leading the ministry's efforts to coordinate the international partners on responses to cyber incidence and cybercrime investigations since January of this year. Among his many responsibilities, he has also remained a crucial voice on issues related to cybersecurity as well as counter terrorism. Welcome ambassador, it is great to have you with us and a pleasure and an honor that you could join us today for this crucial conversation.

But before I turn the floor over to Ambassador Bae for his keynote remarks, a brief

reminder that we're very much on the record today and we're streaming live. And you can submit your questions to events@brookings.edu. That's events@brookings.edu or on Twitter using #ATTFcyber, #ATTFcyber. So, with that, thank you again for joining us today and ambassador, thank you for your commitment and service to your country, your friendship to all of us and for your engaging with us today in this important forum. Sir, the floor is yours. Thank you.

AMBASSADOR BAE: Thank you. It is an honor to be invited to this webinar and I'm glad to share our cybersecurity policy and experience. I'd like to thank Mr. John Allen, the president of the Brookings and Dr. Jung Pak. As one of the most wired countries in the world, the Republic of Korea has been exposed to significant cyber intrusions in the past. From the DoS attack in 2009 to the Korean hydro and nuclear power back in 2014 to the WannaCry ransomware attack 2017, which all served as a wakeup call.

The landscape is constantly shifting. If I take a snapshot of the current state, first the financial sector has emerged as a major target of the malicious acts. Especially, numerous hacking accidents of cryptocurrency exchanges have taken place with a considerable monetary loss.

Second, complex sphere phishing emails have become a matter of everyday occurrence to government officials in charge of national security and foreign affairs. We have learned only in hindsight that larger scale attacks often have stemmed from seemingly minor human errors resulting from social engineering.

Third, the internet of things and AI enabled devices are significantly expanding the threat surface. Experts are wary of an eventuality of massive cyber-attacks through IOT devices and urge a state of preparedness by employing for instance scenario based exercises. From a broader regional perspective, the picture appears somewhat similar. The latest evaluations of Interpol and FireEye indicate that ASEAN and Asia Pacific regions face phishing campaigns, banking malware and ransomware attacks.

Another dynamic in play is the pandemic. COVID-19 has accelerated the speed of integrating our daily lives into cyberspace, compelling us to try to rely more on ICT. And malicious actors are obviously taking advantage of the increased vulnerabilities.

Let me now turn to how Korea is responding. First, at the domestic level and then to

international engagement. To consistently address ever more serious cyber threats, the government mapped out a national cybersecurity strategy last year. This strategy has translated into 100 specific tasks to be a fixed timeframe. Its holistic approach, incorporates the protection of individual rights and the private sector's participation in delivering those tasks.

In terms of structure and governance, we now have the presidential office as a control tower in policy coordination and in handling cyber incidents. And each relevant department is taking a lead role. The National Cybersecurity Center for the public sector, the Ministry of Science for the private sector, and the Ministry of Defense for the military sector.

The protection of critical infrastructure has been our primary concern. We have designated over 400 facilities as critical infrastructure and supervised them among other things by undertaking annual vulnerability assessments. Cybersecurity is, of course, a matter beyond the national boundaries. Our international engagement policy emphasizes contribution to global rulemaking, active engagement in trust building and support for capacity building.

Let me start with the rulemaking. To promote a rule based order in cyberspace, Korea is actively participating in the U.N. working group in close coordination with the U.S. and other like-minded countries. We believe that the current system of international law, including the U.N. Charter, is applicable to states conduct in cyber space.

There are some gaps in interpretation. For instance, we do not have consensus on what amounts to an (inaudible) attack in cyberspace. But the best way to address these gaps is to seek a shared understanding of international law rather than start negotiating a new treaty.

And all states appear to uphold rule based order in cyberspace. Yet the ultimate question for many small and middle sized countries would be how effective are those norms in protecting them from cyber threats. With that perspective in mind, we advocate the duty of due diligence whereby a state should remain vigilant so malicious actors cannot exploit its territory to harm others.

And a confidence building measure is another critical element in enhancing the transparency and stability of cyberspace. At the bilateral level, we have had a cyber consultation with partners including the U.S. Korea is also engaging in trilateral consultation with its immediate neighbors, Japan and China. We are also participating in the ARF intercessional meetings on ITC security at the

regional level.

And one last building block of international cooperation is capacity building for other countries. The COVID-19 pandemic made us realize that no country is safe until all countries are safe. Korea and the U.S., for instance, had a consultation recently to explore any convergence between Korea's New Southern Policy and the U.S.'s Indo-Pacific Strategy in terms of how we can build capacity building over cyber security in this region. With this kind of linking, we can avoid redundancies and enhance the efficacies of our programs.

South Korea, I believe, has comparative strength in cybercrime investigation and forensics. As such, we have helped Bangladesh and Sri Lanka build a cyber investigation center and are working now with Indonesia on building their cyber forensic capacity.

Between states, I think we have to have multiple layers of cooperation in emergency response, information sharing, diplomacy, defense and law enforcement. But as the line between cybercrime and cyberattack is sometimes being blurred, cooperation among law enforcement agencies is becoming more important in shaping those malicious actors' calculation of cost and benefit.

Up to now, I have discussed the cyber threat landscape and how Korea is responding to the challenge at the domestic and international level together with the like-minded countries. We recognize that norms, CBMs and capacity building measures should develop hand in hand to create a virtuous circle. Again, our priority has to be on their implementation putting all three of them into practice.

We must yet admit that technology is outpacing policy and rulemaking. We have demanding challenges related to coping with emerging technologies. Artificial intelligence and other new technology amplify the dangers of malicious cyber activities. Various forms of cyberattacks coupled with disinformation present another difficulty.

Targets are constantly changing and from banks to cryptocurrencies and now also to medical facilities. And most of all, the COVID-19 pandemic has exposed the vulnerability of our multilateral system while our resources are being redirected and exhausted because of the pandemic. Cyber threats continue to evolve with ever increasing sophistication and audacity.

To address these challenges, resilience in isolation will not be enough. We need to step up bilateral, regional and interregional cooperation not just for strategy discussions but also for practical

measures and implementation.

Another lesson from the pandemic is that public-private partnerships are vital in our fight against the virus. Analogies are often drawn between disease control and cybersecurity. And we do not have a global CDC for cybersecurity now and at the moment, it sounds like a distant future. But in terms of rulemaking, consensus making and international cooperation, the multistakeholder approach is instrumental. And I believe this is the only viable path to achieving affective public hygiene in cyberspace.

In that regard too, I appreciate the Brookings Institution's efforts to raise awareness and bring us together with this webinar. I thank you for your attention.

DR. PAK: Ambassador Bae, that was a fascinating discussion about what South Korea is doing and how you see the landscape of cybersecurity. You know, I wanted to spend the next few minutes to talk about what South Korea has done. And you've made this reference between this very interesting comparison between cybersecurity and global health security about the cyber, CDC for cybersecurity as much as we do for pandemics.

South Korea has shown how digital technologies can be successfully used to track cases to contain and treat the coronavirus. But this has justifiably raised questions about privacy and civil liberties. What are one or two key actions that we need to take to ensure against the abuse of digital technologies and protect individual rights during public health emergencies?

AMBASSADOR BAE: Thank you for your question. Korea experienced the MERS outbreak in 2015 and we learned some lessons at that time. And we enacted the law to allow health authorities to collect and disclose certain data under limited situation to make sure the public's right to know.

And this time in our fight against COVID-19, Korea has carried out three T's, testing, tracing, and treatment in a commitment to open this transparency and civic participation. We could resort to this previous law but only in accordance with that law and with the same appropriate safeguards. The premise was, of course, that the government did its best to win trust over the full transparency to fulfill the citizens right to know about every aspect of the spreading disease and government action.

Still in doing so, we seek to make an improvement. To address privacy concerns, the

Korea Disease Control Agency has established specific guidelines on timeframe and scope of publicly accessible information to ensure the necessity and proportionality of those measures. And also, the Personal Information Protection Commission announced the strengthen of the guideline in September for COVID-19 related personal information. And is making continuous effort to improve and implement these guidelines for protection of privacy.

Likewise, I think it is important to have these safeguards in place under the rule of law and also to have open discussion on how to balance between public safety and privacy from the perspective of democracy and human rights.

DR. PAK: Thank you. I wanted to pivot a little bit. You talked about how policy is going to be constantly outpaced by the technology. And, you know, I wanted to ask about ultimately, it's people who are developing these technologies and it's people who are the first line of defense when it comes to cybersecurity. How do we make sure that we're giving the next generation experts the right training to tackle these quickly evolving cybersecurity challenges?

AMBASSADOR BAE: It's like anybody else, it's our priority to foster manpower for cybersecurity. And this is a long-term project and requires conscious and continuous efforts on the part of both government and private sector. And at the moment, Korea has more than 160 universities and other institutes that have departments of cybersecurity, I think where about 9000 are enrolled. And we are supporting these programs, for instance, by designating some of them as a specialized institute of cybersecurity. And also, by encouraging to study the so-called convergence issues like smart cities, smart factories and other IOT enabled projects.

We are also working on the program of the next generation's security leaders to find and foster talented young people in this field, even in high school. And for cybersecurity, I think the next generation might be too late. We need to mainstream this issue with lifelong education and training. And Korea, for instance, designates every July as the month of cybersecurity and holds various events to raise public awareness of cybersecurity. And I believe this is ultimately an issue of investment for the future. Thank you.

DR. PAK: Ambassador Bae, thank you so much for sharing your insight and your experience. This is a great way to kick off our event. Ambassador, thank you for joining us. I know it's

very late in Korea where you are. Thank you.

AMBASSADOR BAE: Thank you.

DR. PAK: Without further ado, we'll jump right into our panel discussion. As Ambassador Bae noted, Asia countries' success with tackling the public health crisis has shown how Asia Pacific is at the forefront of digital technology development. And its population is highly connected and digitally savvy.

Yet as the pandemic has shown our dependence on the internet, it has also exposed our vulnerabilities. Moreover, the quickly evolving cyber landscape has been made more fraught by an increase in cyber-criminal activity as the pandemic has expanded the attack surface and the growing importance of cyber capabilities as instruments of national power and stake craft.

To cover how the region is navigating these issues, I'm very pleased to be joined a panel of distinguished experts. We have Thomas Uren, senior analyst at the International Cyber Policy Centre, Australian Strategic Policy Institute. I think it's around a little past midnight there, Thomas. Elina Noor, director of the Political Security Affairs at the Asia Society Policy Institute here in Washington, D.C. And Mihoko Matsubara, the chief cybersecurity strategist at NTT Corporation. Thank you to all of you for joining us. I know it's very late in Australia and very late in Japan so I'm deeply appreciative of your time.

Tom, I want to turn to you first. Can you talk to us about what are the drivers of malicious cyber activities in the region? What specific actions is Canberra taking to counter them? And can you offer three or four key takeaways from Australia's experience?

MR. UREN: Yes. So, thanks very much for having me. It's a pleasure to be here and it's late but I'm excited to be talking about cybersecurity as usual. And so, your first question, what are the drivers, it works or at least people think it works. So, you know, in the Indo-Pacific, the countries I think of that have engaged in a lot of cyber activity are North Korea, the People's Republic of China and I'm going to stick Russia in there because of Vladivostok just so I've got a bit more to talk about and also the U.S.

So, North Korea, the ambassador spoke about raising -- money being stolen. And so, this is one of North Korea's strategic goals. They want to get power currency, they're using cyber operations to steal money. So, both real money from banks but also money from cryptocurrency exchanges and South Korea has definitely been a big target. So, you know, it's one of their strategic

goals.

The PRC, one example is their goal to promote their own manufacturing industries and advance manufacturing the Made in China 2025 initiative. And cyber espionage has been used to steal a lot of intellectual property. So, that's not the only way that they do it but it's part of their initiative. So, it's contributing directly to their strategic goals.

Russia similarly it's used a lot of cyber operations that it thinks are helping it out. So, for example, part of the state operations has been a state doping program for their athletes. And they've used a lot of cyber operations to not justify it but to when that doping program was discovered to try an undermine what other countries had done sort of to make everyone else look bad. I mean, famously they disrupted the U.S. election last time, 2016, and no doubt they're trying again. So, they're using cyber operations for their strategic goals.

I mentioned the U.S. They've behaved quite differently in that they're relatively transparent about what they're trying to do and they're trying to demonstrate that you can use cyber operations in a responsible way. So, they're a bit different from the other three actors I've spoken about. So, it works.

So, what has the Australian government done about it? I think it's important to note that this is taking place in a context of quite a lot foreign interference in Australia. So, the Department of Home Affairs talks about democratic institutions, education research institutions, media and communications, disparate communities and critical infrastructure. So, that's, you know, almost everything. And cyber operations are one way that other countries can try and gain some advantage.

So, Australia has taken other actions against foreign interference. The cybersecurity parts, we've had a cybersecurity strategy since 2016. So, that's four years now. At the time, there was a special advisor to the PM and one of the important things was a cyber ambassador. And the cyber ambassador went around, particularly Southeast Asia and promoted responsible behavior. We've been relatively transparent in the region. Not as transparent as the U.S. but more so than many other countries about what that might mean.

So, you know, following the rule of law, proportional, you know, necessity, try and limit collateral damage, those kinds of things. And also, and education programs in the region around the U.N.

Group of Governmental Experts' norms.

There are many other things that are in the strategy that you would kind of expect to be in a government strategy. I'll just pull out a few things that may be somewhat different to Australia. In 2017, the government announced the Australian Signals Directorate, the Australian equivalent of the National Security Agency would use offensive cyber capabilities against offshore cyber criminals.

So, I think this is somewhat unusual in that most countries maybe they do it but they don't publicly announce that they do it. And it's almost somewhat at odds against the international law legal use of force in that if it's a law enforcement issue, it really should be up to individual states. But Australia has tried to -- that's actually in legislation that it's got that role.

And I think what the government was trying to do was deter cyber criminals by saying we've got a national authority that will come after you. That's been reiterated during COVID-19 and in the 2020 update, the government announced a whole lot of extra money for the police, the Australian Federal Police to basically enable them to understand criminal targets and be able to do something about them. So, the police don't have a hands-on role but they'll do the sort of background investigative work to find out who and where to attack. And when I say offensive cyber, I mean to disrupt essentially.

One other unusual thing is that the prime minister gave a press conference in June this year where he announced that Australia was being targeted by a sophisticated state-based actor. So, I'm not really aware that other country leaders have stood up and essentially the press conference was just to say yes, we're being targeted. So, I think that was really two things. It was to try and deter the actor which was China although he didn't say so. And the other thing was to try and raise the priority of cybersecurity within Australia.

One of the other trends is that we've moved from a posture of never saying who was responsible ever and very carefully avoiding ever saying who was responsible. To now, we have done four times joint attributions with the U.S. and the U.K. and a number of other countries. So, Russia twice, the North Koreans once and China once.

But we've also seemed to have moved to a posture of what I call unofficial official attribution. So, when the prime minister stood up and said it's a sophisticated state-based actor, there's not too many of them, but I'm not going to say who. In newspapers the same day, there were many officials on

background saying that yes, it's China. So, we've moved from a posture of never saying who was it was ever in any form to now having quite a lot of backgrounding of journalists.

So finally, takeaways. Disruption, I think, works. U.S. Cyber Command has what they call forward defense or there's a different term which escapes me. But the fact that the Australian government is dedicating quite a large percentage of the current strategy to funding there makes me think that it works and it's been worth investing in.

It's not clear to me that attribution has actually deterred anyone. In the U.S., I see the Department of Justice continuing to issue indictments which are one way of publicly naming culprits. And that they're continuing seems to me to indicate that they're not actually having much difference.

One thing the field is evolving the cyber affairs ambassador is now cyber affairs and critical technology. And I think that sort of evolution of technology is becoming more and more important. And certainly, I think of cyber in a very expansive way. It affects many aspects of technology.

And the last takeaway which I haven't really talked about. A 2016 strategy was driven by a prime minister who really cared about cybersecurity. He got deposed and after that, we lost a minister responsible for cybersecurity. So, that role got wrapped up into our minister of home affairs.

And I think having someone who has sole responsibility for the topic is really important because it cuts across so many issues that if you're not trying to pull them altogether, they just get left alone. And I think Australia's strategy drifted for a couple of years. Those are my takeaways.

DR. PAK: Tom, thanks. Can I just ask a quick follow up and you talked about in 2017 and 2020 how the ASD and the prime minister respectively made these statements, right? And that was mostly designed to deter adversaries from doing these attacks. Has that been successful, this naming and shaming or sort of naming and shaming and making those public statements as a way to deter and how would measure that success do you think?

MR. UREN: I think that measurement has been really poorly done in Australia. And so, those particular announcements were designed, I believe, to deter criminals and I just don't think that criminals pay that much attention to what the Australian government says. I think personally they would have been a lot better off just doing it and not telling anyone and the deterrents would come from the fact that criminals talk. They would eventually say hey, something weird is going on whenever we're targeting

Australian people, you know, we just seem to have bad luck, that's weird. Let's go, we'll have better luck elsewhere.

And making us a hard target through operations and actions would have been better than just, well not just talking about it, I just don't think that talking about it helped that much. And I also think it encourages other countries to say well we've got people we consider "criminals" in your country so, you know, it's okay for us to attack them. And I think that's just a bad precedent.

DR. PAK: Thank you. I want to turn next to Elina. You know, the Ambassador Bae from South Korea has mentioned, has talked about these layers, these multiple layers of protection. And you've written several articles about the importance of ASEAN cooperation on cyber issues as one layer of protection. Can you talk about what specific actions the region is taking to build this cooperative infrastructure on cyber issues? What's their relative success and are there three or four key lessons that we can derive from ASEAN's experience?

MS. NOOR: Sure, thank you. I'm going to try to pack as much as I can in the few minutes that I have. Let me do that by offering four brief responses to your questions and then incorporate these takeaways from ASEAN's journey in the cyber realm so far.

The first has to do with taking a step back. ASEAN often gets a lot of short shrift for its painfully glacial pace of movement and that's warranted, that criticism is warranted sometimes. But it's also, in this case, important to step back and consider just how much ASEAN member states have collectively and cooperatively achieved vis a vie cyber issues over the past decade, especially given the diversity of the region.

ASEAN was the first region in the developing world to adopt a harmonized, legal framework for ecommerce. The drive for regional integration and desire to leverage cyber space for economic growth in particular have over the years produced a number of master plans and plans of action. Frameworks related to ICT's, digital connectivity and of late smart cities network, ecommerce, digital integration, personal data protection, so on and so forth.

If you think about the differences in governance systems, technological skill, languages as well as competing domestic priorities set against resource constraints in 10 different countries it's pretty remarkable for this grouping to come so far in such a short time. And I think it's important to keep

that in mind.

Second point has to do with technical capacity. In order to secure this digital drive within the region, all 10 ASEAN member states have now established a computer emergency response team. Of course, the level of technical capacity and resources varies among the countries. But the fact is that all 10 states have conducted incident drills together, some for over a decade.

The most recent iteration of the ASEAN CERT Drill was held earlier this month with an exercise to respond to malicious opportunistic campaigns on the back of COVID-19, so very timely and relevant. Eight of the 10 ASEAN member states are members of the Asia-Pacific CERT. And within ASEAN member states and among themselves, public-private sector incident drills are regularly held.

My third point has to do with policy capacity. In 2018, led by Singapore as the ASEAN chair that year, ASEAN member states agreed in principle to the 11 norms of responsible state behavior that Ambassador Bae mentioned. That was laid out in the 2015 U.N. Group of Governmental Expert's consensus report. ASEAN was the first regional body to do so.

This was a huge step, given that only three of the 10 ASEAN member states have only ever participated in the UNGGE since its inception. And that many member states, indeed many states all over the world are still struggling with even the idea of normative behavior let alone the application of international law and cyberspace.

Beginning this year, ASEAN will work together with the United Nations to develop a norms implementation checklist. So, that member states can keep track of their implementation of these 11 norms as a demonstration of commitment to stability and cooperation in cyberspace.

Now reality check is my fourth point. There are still many, many gaps of course at the technical, policy, operational and legal levels. The region is a hotspot for cybercrime given the steady rise in digital economic activity there warranting greater attention to basic cyber hygiene at all levels from the individual user to organizations and the governments.

There are also cross border coordination and harmonization details to work through as connectivity projects involving critical information infrastructure mushroom around the region. One example that I'm thinking of is the ASEAN power grid.

Additionally, as the discussion rages on in international forums on how exactly

international law will apply in specific situations in cyberspace, ASEAN member states do well to seriously consider these issues individually as states and collectively as a regional group. Taking into account the countries different legal traditions, historical context and future interests in this vast evolving space. Including AI, the internet of everything and everybody.

Fifth and final point is cooperation. Cooperation with dialogue partners outside of the ASEAN region. With the cooperation of regional partners such as Australia, Japan, the United States and, of course, the Republic of Korea, these gaps that I mentioned will slowly be plugged.

South Korea's reputation is one of the worlds most connected nations, as Ambassador Bae mentioned. With a closely integrated digital economy is something that ASEAN member states aspires to. And the country's South Korea New Southern Policy should naturally pave the way for numerous opportunities for Southeast Asian countries to learn from its northern neighbor and for both parties to exchange experiences with each other.

So, in short, let me summarize it all with three words. The ASEAN cyber experience so far has been one, developmental pragmatism, two, incrementalism and three, cooperation.

DR. PAK: Thanks, Elina. Could you elaborate, if you can. You know, Ambassador Bae mentioned capacity building, right. ASEAN is this, you know, covers a huge part of the world, 10 different countries and their cybersecurity practices and capacities and technologies are very different, right. Can you just say a couple of words about what, you know, Singapore for example or other, you know, more technologically advanced countries are doing to boost the capacities of other countries that don't have that capacity on cybersecurity?

MS. NOOR: Yeah. Singapore as you already pointed out has really taken the lead in the region to boost capacity building. Together with the United Nations and other ASEAN dialogue partners, they've set up a number of capacity building programs and training. And similar to that, training has consisted of partners outside of the Asia-Pacific region as well.

So, for example, I and some colleagues from Africa have been involved in exchanging best practices with ASEAN officials in helping to understand what norms mean in effect and in practice in Southeast Asia. And I'd just like to point out that actually a lot of Southeast Asian countries don't recognize this but the 11 norms are already partly in practice. You just don't think of them in the norm's

framework terms.

And so, Singapore has pledged a lot of money for this. They've actually boosted the funding for Cyber Capacity Centre of Excellence. And I think together with these partners that I mentioned, will only continue to work more and more to increase capacity building at all levels, technical, policy, legal, operational, for the region.

DR. PAK: Thank you, Elina Noor. I wanted to finally turn to Mihoko Matsubara to look at some of the private public partnerships. Can you provide one or two specific examples of successful government industry collaboration, including some of the challenges and obstacles and constraints and some key lessons that the U.S. and the region can draw from those examples?

MS. MATSUBARA: Sure, thank you. Because Elina already gave us an example of the importance of our capacity building. So, it's a great segue to talk about Japanese industry-driven public-private partnership to build cybersecurity professionals capacity building.

So, this is a global challenge not only in the United States, Australia, Malaysia or Japan and this is a global issue that we face acute shortage of cybersecurity professionals. Because we are seeing an increasing amount of cyberattacks and more sophisticated cyberattacks. And according to $(ISC)^2$ Cybersecurity Workforce Study in 2019, the world was in short of more than 4 million cybersecurity professionals. And even in the U.S. alone, it was like almost 500,000 cybersecurity professionals was in short.

So, we have a huge gap to fill. And it is even more serious in Japan because Japan is preparing for hosting the Tokyo 2020 summer Olympic games although that now we have to postpone this event till next summer due to this pandemic.

So, back in 2015, major Japanese critical infrastructure companies, namely NTT, (inaudible) corporation and Hitachi decided to launch the Closed Sector Forum to hire or retain trained and educated cybersecurity professionals in collaboration with in the government and academia.

But to do that, the first task they need to tackle with was to find a global common language to communicate with each other. Because these members, the country the forum has 43 members as of today and they are from totally different critical infrastructures like manufacturers, transportation, media or chemical. So, they obviously have totally different business practices, totally

different expectation for cybersecurity.

So, they need to find, okay so what is cybersecurity professional means because it can be anything. Even though it's a very simple term to say cybersecurity professionals, can talk about cybersecurity policy analysists at ASPI or Brookings or if you talk about cybersecurity network analyst at NTT. We are totally different professions.

So, that's why they said okay, we really need to have a common ground but we need to go to a global standard rather than the Japanese domestic one. Because first, all of the forum members have a global business presence and also the 25% of the forum members the Tokyo 2020 partners.

So, they sort of it's better to have a global common language to communicate with and also define what kind of cybersecurity missions they need to pursue and what kind of expectations for each type of cybersecurity appropriate needs to have and what kind of skill set they need to have and what kind of level of (inaudible) they should have. It's better that because they can bring back their findings on discussions on best practices back to the subsidiaries not only in Japan but also outside Japan.

So, they ultimately decided to choose the NIST Cybersecurity Framework, National Institute of Standards and Technology in the United States. Why? Because the NIST Cybersecurity Framework is not only for the United States but it's a global standard. And B, the Japanese government already provided the Japanese translation of this document. And some of the forum members already talking to the team were already familiar with the contents of the NIST Cybersecurity Framework.

So, they decided to go to the NIST Cybersecurity Framework to define, okay so what kind of cybersecurity mission is Japanese critical infrastructure companies need to fulfill and what kind of cybersecurity skill sets are needed to fulfill each type of profession and what kind of level of deepness of understanding.

For example, if you are CISO like chief information security officer, you are expected to know about some level of understanding on the legal issues not only in Japan but also in the United States, for instance. But if you are, for instance, like database maintenance guy or engineer, you should know some level of understanding on legal issues but not that as deep as the CISO should know about legal issues.

So, the forum decided to map out the different types of appropriations and the skill sets

on the deepness of understanding. And also, mapped out the calendar to this type of cybersecurity profession needs to do this kind of task between this month and this month. Although you cannot expect when cyberattack will really happen but you have some routine tasks to do like budgeting or auditing.

And some of the forum members started to sponsor cybersecurity courses at different Japanese universities. And also, they started to send their employees to those universities to share their hands on first hand experiences to how to tackle with cyber-attacks with university and graduate students.

These types of efforts of the forum members started to (inaudible) the indication from the Japanese government strategy committee meetings from different ministries and agencies to make sure to incorporate industry voices into policymaking on how to develop cybersecurity deterrents. And back in 2018, actually the Japanese national level of strategy and policy started to defer to the cross-sector forum name and also publications to how to develop cybersecurity professionals.

But these kinds of efforts have not been done without any bump. And, of course, it was all sorts of trials and errors. Because possible it's very old cliché but Ambassador Bae also mentioned the importance on trust, on confidence building. Because if you don't have trust with other members on the forum, you really don't want to talk about your own internal programs like breeches and what kind of cybersecurity you're dealing or what kind of cyber defense that you are implementing.

So, it took several months for the forum members to really feel comfortable to talk about their internal issues with other members. And also, they started to talk about not only how to develop cybersecurity professionals but also, they started to talk about how to deal with cyberattacks and cyber threats.

And so, to summarize and also to share some best practices and lessons learned from this cross-sector forum with other countries, United States and Australia and Malaysia and other countries. I think that there are at least five actions to take to have a successful public-private partnership or a public-private academic partnership.

So, first action you should take is to find a common language to make sure that you have that affective and efficient communication with other members. Because maybe your members have a different background, different expectations for cybersecurity.

And second, you should make sure to meet up on a regular basis. You should have a

routine. Otherwise because everybody on that kind of forum or framework is really busy with their day to day work because there are always bad guys out there and you have to deal with tons of cyberattacks. So, you have to really have regular meetings.

And the third task you should have is to make sure that you identify and prioritize at least only a couple of important topics that everybody would agree to talk about. Everybody is interested in talking about. Otherwise, there would be no value to bring it back to the members' employers. Because unless the senior leadership in each of the senior leadership on their company, they will not support you to go to the forum meetings and using their business hours to talking to your competitors. So, make sure you have something valuable to bring back to your organization. But it takes time because you need to take time to make sure that you have a trust.

The fourth action you should take is find a couple key people who are well respected in your own local community. Everybody will say that yes, you really should listen to this person. She's great or he's great to listen to. Otherwise, it is very difficult because different people have different opinions and different priorities. So, if the key people say that yes, I'll make sure to make my time available for you, to make sure to coordinate everybody's different concerns and priorities and interests. So, that we should make sure to prioritize our tasks to tackle with cyberattacks or capacity building.

And last but not least is to make sure to build a culture that a free ride is not acceptable. Because everybody wants to take advantage of this kind of public-private partnership or information sharing. Everybody would agree that yes, information sharing is important but usually people just want to just take it out, not give it back to the community. So, make sure that you have to bring it back to your own community or your own forum or in the public-private partnership and everybody will speak up about their own experiences.

However, I'd like to also mention about our original discussion on the COVID-19 pandemic impact of our daily lives and on the research and the work. Because it is getting really difficult for us and also, it's been a really weird year for us to not having the face to face meetings anymore. It's been really leery to have those kinds of meetings. And cybersecurity professionals are kind of paranoid to talk about sensitive issues with strangers especially over online or the internet.

So, unless you have some level of understanding or trust, it will be very difficult to have

meaningful discussions of any types of public-private partnerships or public-private academia partnership on cybersecurity. Because cybersecurity is all about trust and it can be very sensitive. Thank you.

DR. PAK: Thanks, Mihoko. I'm reminded, we had David, we had a conversation with David Koh is the chief of the Singapore Cybersecurity Agency and what he said was really so appropriate. He said that, you know, most people know how to be secure in their own homes. You know, they lock their door, or they'll close their windows and they have their keys with them at all times. So, they know how to be safe at home with their physical security.

But when it comes to cybersecurity, people don't know. And I think, Elina and Mihoko, you talked about how training needs to be a part of this culture of cybersecurity and building it from the ground up.

So, I wonder, you know, if I could, Mihoko, you talk about the common language, right, a common language, common set of requirements. How do you square the circle when you have diversity, when you have, you know, relative silos? And you've brought up trust and Elina has brought up trust and I think Tom has brought up trust as well. These are very human emotions. You know, there's a psychology involved in all of that.

And so, categorizing or kind of having a structured way of looking at security, the 11 norms, right, Elina that you mentioned, a checklist. What are the requirements? What sets of training? How do we even start? Or how do we -- can you tell us about those norms? And Elina I welcome your comments too. Those norms or that common language to, you know, to make sure that we're all speaking the same language.

MS. MATSUBARA: Yeah. So, when you talk about cybersecurity or cyberattacks to long IT cybersecurity people, it is always better to bring up some specific examples of damages caused by cyberattacks. And sometimes it's very difficult for people who can imagine about what kind of damages can be caused by cyber espionage. Because some people are really humbled to think that we don't really have secret information. It's okay, nobody will attack us by cyberattacks.

But they don't just realize how valuable information or assets that they can have. So, it's better to talk about something with more specific and more visual like ransomware attacks because it encrypts your data and it holds your business operations as hostage. So, you can see what kind of damage already caused by a ransomware attack.

So, if you show this example like hey, so this organization, like this hospital was attacked by this ransomware attack and actually it already happened. It was a tragedy that a female patient simply 8 years old was killed due to a delay in her transfer to a different hospital after the ransomware attack taking down IT services in the university clinic.

So, this type of example is really relevant especially during this pandemic. We really need to have a 24/7 access to medical services. And if we do this kind of precious and much needed access to critical infrastructure services then people would say yes, now I get it. We really need to have some security to make sure that we can access to these types of operations.

DR. PAK: Elina or Tom if you had any follow up comments on that.

MS. NOOR: Yeah, I'll just make a couple of points if I can. I think this issue of trust that Mihoko highlighted is an important one because it contributes to the creation of a common language. And Jung, you mentioned that this is a human emotion and a sentiment that is cultivated, I think, through regularized communication and meetings.

You know, ASEAN is often criticized as being nothing but a talk shop, nothing more than a talk shop. But I think there is value in that talk shop in that it creates this predictability and stability of communication. ASEAN has over a thousand plus meetings a year so it's sheer craziness. But at the same time, it creates this regularized schedule of meetings that instills this trust that can go towards making a common language creation much easier.

Second point that I'll mention is that the idea of putting forward cybersecurity strategies from countries within ASEAN helps with this common language. So, that at the very least, what you have is a comparison of these different strategies and plans and then you can begin to discuss some of the terminology in there and what it means and whether the understanding of these different terms can be merged into some sort of common understanding.

MR. UREN: So, it's late in Australia. I'll just try and be a bit controversial at this point. And I'm actually quite skeptical of norms the way that they're talked about. So, people often talk about norms as if they're the be all and end all of achieving peace. And the problem I see is that you get to norms when there are actually punishments, essentially for transgressing them.

So, I'm wearing, you know, a suit and a shirt. If I turned up wearing nothing at all, I

wouldn't be on this panel anymore. I've transgressed a norm and I would have been punished. And I think with right now what I see is that cyber operations, the benefits outweigh the costs and people will continue doing them.

And so, of those 11 norms, I think the ones, many of them everyone agrees to and will just do because they make sense. And the ones that aren't agreed to, the benefits outweigh the cost and they won't change. Elina and Mihoko spoke a lot about trust and meetings and I think they're great.

So, in the absence and I would describe them as confidence building measures is another term people would use. And in the absence of an agreement on how to behave, at least being able to talk, I think, is really worthwhile because at least then you've got the chance or the likelihood that you avoid unintended mistakes.

DR. PAK: Thank you. You know, one of the things that I really appreciate about having voices, experts from the region to talk about various issues is that, you know, not everything is about us, the U.S. And so, while the U.S. has come up every now and then in this conversation, you know, it'd be great to get your perceptions or views and assessments from where you're sitting and the countries that you cover on what kind of role the U.S. plays. In either providing leadership or hampering cooperation, or encouraging cooperation.

You know, if you could talk about, you know, how does the U.S. fit into all of these efforts that you're talking about? I mean, these have been really multilayered, regional, intraregional or national based. So, can you bring the U.S. into this conversation and talk about from where you sit what kind of role the U.S. should play or has been playing? Maybe I can start with Tom.

MR. UREN: So, when you started asking that question, the thing I immediately thought of us was Huawei and ZTE and the recent Clean Networks Initiative. So, the background to that and I didn't talk about this before is that Australia first banned Huawei from our national broadband network back in 2012. So, that was a fiber network that was being rolled out to much of Australia. So, we actually have a really long history of considering the security risks of Chinese vendors going way back.

But my observation was that when the U.S. started to get involved, and I think this is a lot to do with the way the Trump administration behaves. It felt like many countries in the region were feeling that their arms were being twisted. I mean frankly, they don't like it. And it seems to me that the Clean

Networks Initiative is trying to achieve the right thing for the right reasons but just in the wrong way.

And it seems to me to be too directing, trying to direct people rather than trying to convince them and bring them along. And I think the power of the United States has always been in the attractive power of the, you know, the beacon on the hill, the sort of American exceptionalism. And it's just not -- your administration is not being very attractive right now. So, that's probably the kindest way I can say it.

DR. PAK: So, let me follow up a little bit, Tom. And what are the consequences of that? What are the consequences of that kind of arm twisting, what kind of position does that put Australia in and is there harm caused?

MR. UREN: Oh, there's definitely harm, yes. And I think it's not irrecoverable but people have, particularly around Huawei and Chinese vendors, it's kind of a cost versus some theoretical benefit. And if people are not expressing that theoretical benefit in a way that really makes sense or in a way that's attractive, that pulls you in, I guess I would rather have a really good salesman rather than a really good arm twister. And the administration right now seems to be more, you know, come with us or else. And I just don't think that that wins friends and influences people.

For Australia, we're, I think, in a very difficult situation in that we've tried to balance our security partner, the U.S. with our biggest trading partner which is the People's Republic of China. And that has really polarized that relationship more so than it was before. And so, we're facing a difficult problem where one of our biggest intelligence adversaries is also our biggest trading partner.

And having the U.S. be so anti-China and anti-Communist Party makes it very difficult. And I don't think we're really figured out how to deal with that. I mean, we're trying to build alliances with other countries in the region, I'm sure, but I'm not sure how well that's going.

DR. PAK: Elina, any thoughts?

MS. NOOR: Yeah, I'm going to take up Tom's challenge and be slightly provocative. And your question is certainly quite provocative so let me take up that challenge. I would agree with what Tom said. But I would also add that there's a lot of talk about a rules-based order in cyberspace from working on stability of cyberspace.

And these are all principles that small states, particularly around the world but in the

ASEAN region adheres to and would like to see preserved. Because international law is supposed to be the equalizer of powers in theory. Right, we all know that's not true in reality.

But so far as it is a framework, you know, I think Tom mentioned the U.S.'s concepts of defend forward and persistent engagement. These ideas really push boundaries quite literally because the idea of defending the U.S. beyond its borders and moving into other countries borders where necessary. And as the U.S. sees fit, really undermines this whole idea of not only stability and a rules-based order but also trust.

And it hampers capacity building efforts because then the question of the sincerity of the U.S. and lending support becomes an issue to what end. And countries in Southeast Asia are not naive. You know, we don't expect a free ride. As Mihoko said, we understand that there are realist interests at play.

But at the same time, as Tom said, countries don't want to be pushed in one direction or another. And to have these kinds of concepts floating around and practices in play makes it very difficult to come to an understanding of what a rules-based order means and whether it applies equally across the board.

DR. PAK: Mihoko, do you have any comments to follow up?

MS. MATSUBARA: So, I think the United States has been really relevant to these types of discussions on the capacity building, especially in the ASEAN countries over the last decade or so. So, it is not only unilateral efforts to help out ASEAN countries on capacity building but also it can be bilateral. So, I can give you some examples.

So, the United States has been really active to provide capacity building support for ASEAN government officials on cybersecurity. And the U.S. government has been also closely walking with the Singaporean government to provide different types of capacity building support, including cybersecurity.

And I'm very pleased that our cybersecurity capacity building efforts have been really getting a lot of attention. And not only attention but also actions, specific actions from different government. From Australia, the U.K. and also Japan. And sometimes under those countries are bilateral efforts to coordinate different types of capacity building support for ASEAN countries.

So, I think this is great to make sure to close the gap in terms of the acute shortage of

cybersecurity professionals and also to have direct face to face conversation between the different countries to tackle with cyberattacks. And also, to make sure to be on the same page in terms of how to prioritize on cybersecurity. Because as you said and also Ambassador Bae mentioned that the cybersecurity is a multifaceted issue and we have different priorities to deal with cybersecurity.

So, it's not just that every country has different opinions and priorities about cybersecurity. But it is great that not only the United States and Australia and Japan and Singapore have been really closely walking together to tackle with cybersecurity and capacity building.

DR. PAK: Thank you. I want to ask one more question before I turn to one or two audience questions. I remember, you know, I used to work at the Office of the Director of National Intelligence back when Jim Clapper was the DNI. And I remember back in, I think it was 2013 when he said that, you know, when cyber outranked everything else, all the other security threats to the United States. And he specifically said, we're not looking at Pearl Harbor type event.

And I was struck by how Ambassador Bae talked about, you know, that we should be prepared for this massive Pearl Harbor type of event in terms of this huge assault that could lead to a conflict. How much does that kind of scenario keep you up at night and if I could go to one audience members question, is it China or Russia? This is coming from Gordon Johnson, a member of our audience. Is it, you know, when you think about these massive potential cyber events that could lead to a conflict, are we looking at China or Russia?

MR. UREN: Okay, I'll go first. Does it keep me up at night, mostly no. So, the most compelling worry I've had said to me is that something happens by accident that is actually tremendously damaging, some sort of worm. And I guess that is kind of similar to what NotPetya was like or perhaps the (inaudible) or the Morris Worm back in the day. And it's kind of the 'no one with the exception of the Russians,' no one deliberately releases things that spread like that.

And that's the whole point of why Australia about responsive behavior and the U.S. has been transparent about how they try and be proportionate and avoid collateral damage. So, mostly it doesn't keep me up at night.

I think China also has, most of its efforts have been to try and promote China as central in the world order. And so, it would seem to be counterproductive to launch something that's just

tremendously damaging randomly. I guess there's kind of offhand undesirable scenarios like a conflict over Taiwan that maybe changed that calculus. But that right now, I would say that Russia more likely to do something kind of semi-deliberate accidentally where they just don't pay enough attention. China, not likely at all.

DR. PAK: So, there's a self-imposed constraint system, this reputational risk that would prevent or constrain a nation state from some catastrophic incident or initiating a catastrophic incident.

MR. UREN: I think the problem with a catastrophic incident is that it results in catastrophic payback. So, if it were bad enough, people would respond in other ways. And I think both China and Russia, well no one wants to escalate anything ever from cyberspace to anything else.

But I think if people were pushed hard enough, they would. They'd have to be pushed really, really hard but I don't think, you know, the entire dynamic of why cyberspace is useful is that people don't escalate into other realms really at all. So, I think there's that dynamic on one side and the other side there's an incentive not to push people to far because you never know where that boundary actually is.

DR. PAK: We have just a couple more minutes left. I want to turn to a question from the audience. Albert Hong from Radio for Asia. In case of North Korea, Tom, you mentioned this before. The hacker groups are secretly working in foreign countries but the countries seem unable to properly crack down.

And Tom, you mentioned the idea of, you know, when is this a law enforcement issue and where are the boundaries? Is there really any way to stop North Korean hacker groups' activities, how is cooperation with the countries involved? Maybe I'll direct this to Tom and then Elina.

MR. UREN: That's a good question actually. I'm not 100% an expert on those on why they survived. I think partly there is many North Korean hackers in the PRC and I think that's partly because the PRC realizes that cutting them off would actually be perhaps too damaging for the regime.

So, there's my take is that there's kind of a love-hate relationship with the regime and Pyongyang and we like them more than the South Korean's on our border but we don't like them too much and we don't want them to collapse. So, they're kind of stuck between a rock and a hard place and it's kind of managing there as a -- and I think cutting off their cyber capability might lend too much towards collapse which is terrible for the Chinese. I'm not so sure about the Malaysians. Perhaps Elina or Mihoko might

have a better idea. So, I know that there's North Koreans in Malaysia as well.

MS. NOOR: Yeah, I think and this sort of goes back to Jung's earlier question about China and Russia as well. Their threat deception in Southeast Asia is quite different from that elsewhere. There's no declared adversary and, you know, countries in Southeast Asia including Malaysia have diplomatic relations of some sort with countries like North Korea.

So, I think the threat is not so much from the outside as seen within Southeast Asia because of the composition, the diversity and the multiculturalism of many countries in Southeast Asia, the threat really is from the inside out. And we haven't touched on this very much during this discussion but as I see it, content is a huge concern within Southeast Asia.

This idea of misinformation or disinformation campaigns in Southeast Asia that undermine the social fabric of countries in the region is seen as a much, much bigger threat than that coming or emanating from other countries in other parts of the world.

DR. PAK: Thank you. You know, just to wrap up, you know, North Korea really enjoys to have a permissive environment and they use those diplomatic engagements and diplomatic relationships with various countries, especially in Southeast Asia and China to launch their activities. And I think Tom, you're right that it, you know, it doesn't from China's perspective it doesn't hurt anybody. You know, there's no lethal maneuver but that, you know, if it's a minor nuisance from Beijing's perspective.

You know, we have run out of time. I just wanted to thank all of our speakers, especially Tom and Mihoko for staying up very late to have this conversation with us. And Elina, thank you so much and welcome to Washington. Thanks to all of you for your insights, to Ambassador Bae for his insightful comments. So, thanks to all of you in the audience for joining us today. Take care.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative

or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020